empenoso
18 дек 2025 в 10:25

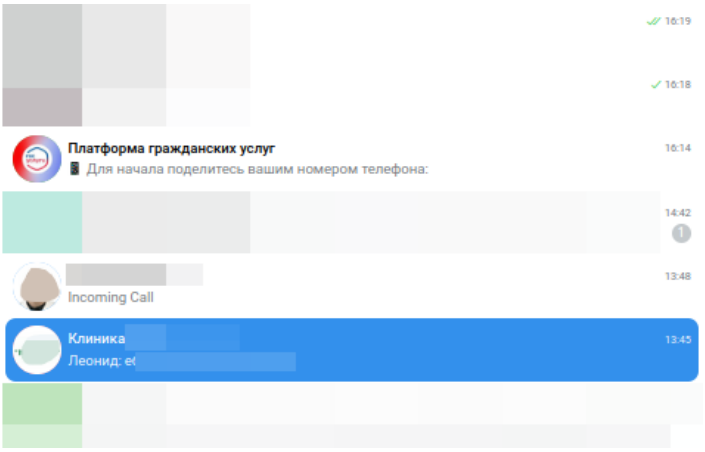
Это не развод: как выглядит современная атака социальной инженерии через «рабочий чат»

Простой 12 мин 53K

Информационная безопасность*, Финансы в IT

Кейс

В понедельник в 13:01 мою маму добавили в рабочий чат в Telegram.
Группа называлась точно так же, как клиника, где она проработала больше десяти лет уже будучи на пенсии и из которой уволилась около пяти лет назад.



Скрин списка чатов Telegram

В чате были знакомые фамилии с реальными фотографиями, а ещё деловой тон, обсуждение «приказов Минцифры», «стажа» и «пенсии». А уже через сорок пять минут этот же чат превратился в поток угроз, оскорблений, фейковых уведомлений о входе в «Госуслуги» и попытку оформить на неё десятки микрозаймов.

Ни один рубль украден не был — но не потому, что схема не работала.

То, что я увидел в этот день, было не просто мошенничеством. Это была тщательно срежиссированная постановка: фальшивые коллеги, заранее подготовленные диалоги, правильная терминология, давление авторитетом и временем. Слово «оцифровка» стало наживкой. «Госуслуги» — оружием. А страх потерять стаж, пенсию и «оказаться вне реестров» — рычагом.

Но эта история — не про деньги. Это история о краже личности в прямом эфире. О том, как за считаные минуты человека лишают ощущения безопасности, контроля и достоинства. Я пишу её не как айтишник. Я пишу её как сын, который в реальном времени вытаскивал мать из цифровой ловушки — и понял, насколько беззащитными мы все оказались перед новой формой насилия.

Дальше — по шагам. Без эмоций. Только факты, механика и выводы для того чтобы в следующий раз вы сами такой чат сразу просто закрыли.

Акт I. Театр марионеток (время 13:01 – 13:23)

Этот этап — самый важный. Здесь ещё никого не грабят, не пугают уголовными делами и не просят «срочно перевести деньги». Здесь строят сцену. Аккуратно, методично, почти незаметно.

Вход в доверие через «работу»

Всё начинается с добавления в закрытый групповой чат Telegram. Не личное сообщение, не звонок, а именно рабочая группа.

Название группы совпадает с реальным названием клиники. Не «что-то похожее», не с ошибкой в слове, а ровно так, как она называлась в документах и на табличке у входа. Почти сразу появляется сообщение от «администратора». Тон — вежливый, деловой, без суеты. Никаких ссылок, никаких требований. Просто задача. «Надо проверить списки». Всё максимально буднично.

Скрин первого сообщения администратора

Использование реальных данных

Дальше в чате появляются списки. Полные ФИО. Реальные даты рождения. Имена людей, которые действительно работали вместе много лет назад. Участники чата отвечают — коротко, по делу: «верно», «подтверждаю», «всё правильно».

Аватары — с фотографиями этих люд��й. Для человека без паранойи это выглядит убедительно. Для человека старшего поколения — почти неопровержимо.

Психологические крючки

Только после этого в разговор осторожно вводятся триггеры. Очень аккуратно, без давления:

- «Удаление из архива»
- «Чтобы не было проблем со стажем»
- «Были случаи, когда урезали пенсию»
- «Приказ сверху, по линии Минцифры»

Скрин чата с этими формулировками

Обратите внимание: ни одного слова о деньгах. Ни переводов, ни карт, ни «безопасных счетов». Только бюрократия.

Это хорошо поставленный спектакль, где жертву сначала делают участником «рабочего процесса», а уже потом — объектом атаки. Пока человек думает, что он сотрудник, а не цель, защита отключена.

Акт II. Технический капкан (время 13:23 – 13:27)

На этом этапе спектакль резко меняет декорации. Если в первом акте зрителю показывали «работу», то здесь на сцену выводят «технологии». И это важно: для человека, который хотя бы краем уха слышал про IT, слово «бот», «подтверждение», «ключ» звучит убедительно. Кажется, что дальше начинается не психология, а техника. На самом деле — это всё та же постановка.

Фальшивый «официальный бот»

В чат выкладывают ссылку на якобы официальный бот «Госуслуг». Название выглядит почти безупречно: @GosUslugi. Глаз цепляется за знакомое слово, мозг дорисовывает остальное сам.

Название бота в чате (@GosUslugi)

Реальный username в профиле (@Di24gubBot)

На деле ссылка ведёт на сторонний бот t.me/Di24gubBot. Но чтобы это заметить, нужно либо специально проверять, либо уже быть настороже. Это не взлом. Это UI-обман.

Эффект толпы в действии

Дальше включается социальное давление. «Коллеги» начинают задавать вопросы: что нажимать, куда заходить. Почти сразу другие «коллеги» отписываются: «получилось», «пришёл код», «отправила».

Скрин общего чата

Самое важное — всё происходит публично, в общем чате. Не в личке. Не скрытно. На глазах у всех. Это классическая техника: если десять человек уже сделали одно и то же — значит, это безопасно.

Мозг экономит энергию и отключает критическое мышление. Зачем сомневаться, если «все прошли»?

Что произошло на самом деле

С технической точки зрения произошло простое действие: пользователь нажал «Поделиться контактом» и передал номер телефона боту. Никакого взлома, никакого «доступа к Госуслугам» в этот момент не было.

Так называемый «код», который просят отправить в чат, — не код доступа и не подтверждение входа. Это элемент спектакля. Реквизит, создающий ощущение процесса и контроля.

Ключевой вывод здесь неприятный: все персональные данные у мошенников были ещё до начала атаки. Этот этап был нужен не для получения информации, а для психологического переключения жертвы — из роли «сотрудника» в роль «объекта операции».

Технический капкан захлопывается тихо. И именно поэтому он работает.

Акт III. Срыв масок и шоковая терапия (время 13:42)

Этот акт — самый короткий по времени и самый разрушительный по эффекту. Сценарий, который полчаса выстраивали аккуратно и почти интеллигентно, ломается за секунды. Маски сбрасываются демонстративно. Именно так и задумано.

Мгновенная трансформация

Вежливый «кадровик», который ещё недавно писал канцелярским языком, исчезает. Его место занимает поток агрессии. Мат. Оскорбления. Троллинг, рассчитанный на максимальное эмоциональное зацепление. Сообщения летят одно за другим — быстро, без пауз, без логики.

Это выглядит как истерика. Но это не эмоции. Это инструмент.

Скрин агрессивных сообщений

Унижение здесь показательное: «ты уже всё потеряла», «мы всё видим», «ты сама виновата». Человека не просто пугают — его лишают опоры, статуса, роли. Он больше не «сотрудник». Он — объект давления.

Цель психологического удара

Задача этого этапа проста и цинична: вызвать панику. Не страх — именно панику. Состояние, в котором мозг перестаёт анализировать и начинает действовать рефлекторно.

В этом состоянии человек:

- не проверяет факты
- не читает мелкий текст
- не сомневается
- срочно ищет «живого человека», который скажет, что делать

Именно поэтому следующий шаг — звонок. Не чат, не бот, не сообщение. Голос. Прямая линия давления.

Фейковые «уведомления»

Параллельно в чат и личные сообщения начинают сыпаться «уведомления»:

- «Вход в Госуслуги с iPhone 16»
- «Геолокация: Украина, Днепро��етровск»
- «Загружена генеральная доверенность»

Одно из сообщений бота

Технический скрин фейкового уведомления

Формулировки подобраны идеально. Современно, страшно, «технически». Расчёт на то, что человек не знает, как именно выглядят настоящие уведомления, но понимает общий смысл.

В МФЦ в 15:16

Когда я с мамой в 15:16 сидя уже в МФЦ узнали:

- входов в «Госуслуги» не было (на фото мой вход сразу когда я оказался рядом с мамой)
- доверенностей не оформлялось
- никаких действий не происходило

Но в 13:42 это знание недоступно. Потому что шоковая терапия работает только здесь и сейчас. И именно в этот момент система либо ломает человека — либо даёт сбой.

Акт IV. Сценарий Б: кредитная бомбардировка (время 13:53 и следующие сутки)

Когда шоковая атака не ломает человека сразу, у мошенников включается запасной план. Он менее эффектный, но куда более изматывающий. Это атака не на эмоции, а на выносливость.

Массовая подача заявок в МФО

В ход идут уже имеющиеся данные: ФИО, дата рождения и номер телефона — все эти данные были у них и до атаки. Этого достаточно, чтобы запустить автоматическую рассылку заявок в микрофинансовые организации. Никаких разговоров, никаких «подтверждений личности». Просто скрипт, который отправляет десятки заявок в разные МФО.

Важно понимать: это не точечная попытка украсть деньги. Это ковровая бомбардировка. Расчёт на то, что хотя бы где-то система даст сбой, скоринг будет лояльным, а кредит — одобренным.

Поток СМС как оружие

Через несколько минут начинается вторая волна — СМС. Десятки сообщений подряд. Коды подтверждения. Уведомления «заявка принята», «заявка одобрена».

Пример СМС

Представьте, что вы получаете около двадцати таких сообщений за короткое время. А теперь представьте, что вам 72 года. Телефон вибрирует без остановки, каждое сообщение — про деньги, долги, обязательства.

Пример СМС

Количество здесь — ключевой фактор. Не важно содержание каждого отдельного сообщения. Давление создаёт сам поток. Срочность, множественность, ощущение, что процесс уже идёт и его невозможно остановить.

Пример СМС

Почему деньги не украли

Деньги не украли не потому, что схема была слабой. А потому что в этот раз система дала сбой — с их стороны.

Пример СМС

Мы быстро доехали до МФЦ. Был оформлен самозапрет на кредиты. Запрет на сделки с недвижимостью был установлен заранее — ещё до этой истории, как мера «на всякий случай».

Сценарий Б рассчитан на то, что человек устанет раньше, чем разберётся. И именно поэтому он опасен. Он не пугает — он давит до тех пор, пока не сломает.

Чёрный список: технические следы атаки

Этот раздел — для поисковых роботов, специалистов по безопасности и тех, кто прямо сейчас гуглит подозрительный номер или ссылку. Я оставляю эти «цифровые отпечатки» здесь, чтобы разорвать цепь анонимности. Скрипты меняются, но паттерны и идентификаторы часто живут дольше, чем фальшивые аккаунты.

Технические артефакты атаки:

1. Фейковый бот «Госуслуг»: внешне он копирует дизайн, но его username выдает подделку: @Di24gubBot (ID: 8279304015). Обратите внимание на механику: ссылка содержала start=aladin... — это реферальный «хвост», по которому скрипт понимает, какую именно жертву нужно обрабатывать.
2. Аккаунты-кукловоды: имена и фото украдены у реальных людей. Но Telegram ID — это уникальный цифровой паспорт аккаунта, который не подделать.
    3. ID 8571326145 — координатор атаки. Сначала втирается в доверие, затем оказывает давление, в финале — глумится над жертвой.
    4. ID 8279304015 (Бот) — фальшивые «Госуслуги». Собирает номер телефона и перехватывает код авторизации Telegram.
    5. ID 5081257726 (Группа) — создана исключительно для спектакля.
    6. ID 8593742198 и 8578455336 — отыгрывают роль коллег, которые «уже всё прошли». После взлома жертвы мгновенно меняют тон на издевательский («доверенность загружу», «паспорт выгружу»).
    7. ID 8438081199 — аккаунт-скрипт, который молча добавил жертву в группу в самом начале (действие invite_members).

Если вы видите эти ID в своих логах или черных списках — блокируйте.

Серые лидогенераторы: похоже большая часть сайтов из списка ниже — это не сами кредиторы, а агрегаторы. Они собирают персональные данные и перепродают их реальным МФО, создавая лавинообразный эффект спама.

Ниже приведен список доменов и отправителей — их системы были использованы в автоматизированной рассылке заявок без согласия жертвы. Если вам пришло СМС от этих сервисов без вашего запроса — ваши данные уже «прогоняют» по скрипту. Хотя некоторые из сайтов (например, nadodeneg.ru) — легальные МФО, зарегистрированные в реестре ЦБ.

Эту таблицу создал я, чтобы обзванивать все организации в день сразу после атаки. Чтобы написать официальные письма или нанять юриста для взаимодействия по мошенничеству.

Но как оказалось многие из них даже не имеют телефона на сайте.

№	Адрес из смс	Сайт	Телефон с сайта

1.	nadodeneg	https://nadodeneg.ru/	88002220224
2.	0-cash.ru	https://0-cash.ru/	ИНН: 645322546902
3.	denginadom	https://denginadom.ru/	8 (800) 770-05-40
4.	bistrodengi	https://bistrodengi.ru/	+7 495 725 25 25
5.	webbankirru	https://webbankir.com/	8 800 775-54-54
6.	budgett.ru	https://budgett.ru/	8 (800) 555-99-80
7.	you-zaimru	https://youzaym.ru/	+7 (499) 340-02-42
8.	valupro.ru	https://valupro.ru/	ИНН 770100251210
9.	sravniza.ru	https://sravniza.ru/	+7 (999) 999-99-99
10.	denga4u	https://denga4u.ru/	ИНН 7816728534
11.	finmanyru	https://finmany.ru/	ИНН: 645322546902
12.	top5-mfo.ru	https://top5mfo.ru/	нет информации
13.	mfonly-ru	https://mfonly.ru/	ИНН: 645322546902
14.	pyblidom	https://pyblidom.ru/	ИНН: 645322546902
15.	bugetut	https://bugettut.ru/	ИНН: 645322546902
16.	na-schetru	https://www.na-schet.ru/	ИНН: 645322546902

Многие имеют юридическую привязку к ИП, зарегистрированному менее года назад.

Было ещё несколько, уже на следующий день пришли.

Что делать, если вы попали в такую ситуацию

В информационной безопасности есть понятие — план реагирования на инциденты. Когда атака уже началась, эмоции — ваш враг. Действуйте по сухому алгоритму. Это чек-лист для минимизации ущерба.

1. Не кормите тролля

Как только вежливый тон сменился на угрозы, мат или требования — **немедленно прекращайте диалог**. Не пытайтесь оправдываться, не шутите в ответ, не угрожайте полицией. Любая ваша реакция дает злоумышленникам время и информацию.
Ваша задача — разорвать соединение. Блокируйте пользователя, выходите из группы, удаляйте себя из чата.

2. Изоляция периметра: не звоните «в поддержку»
Номера телефонов, которые вам подсовывает фейковый бот или присылают «коллеги» в чате — это **SIP-телефония мошенников**. Позвонив туда, вы попадёте не в службу безопасности, а на второй уровень социальной инженерии, где вас «дожмут» голосом.
Настоящая поддержка Госуслуг или банка никогда не звонит через мессенджеры и не просит диктовать коды.

3. Поход в МФЦ
Если вы передали код или перешли по ссылке, считайте, что ваша цифровая личность скомпрометирована.

- **Срочно идите в МФЦ.** Ваше физическое присутствие с паспортом — это «мастер-ключ», который перекрывает любой удаленный доступ.
- В МФЦ сбросьте пароль, настройте вход по TOTP и, главное, запросите историю входов. Убедитесь, что там нет посторонних устройств.

4. Превентивные патчи безопасности
Эти действия нужно выполнить всем, не дожидаясь атаки. Это ваша «цифровая прививка»:

- **Самозапрет на кредиты.** Оформляется через реальные Госуслуги. Даже если мошенники украдут ваши данные, автоматический скоринг отклонит заявку.
- **Запрет на сделки с недвижимостью без личного присутствия.** Это закрывает уязвимость с продажей квартиры через украденную или поддельную ЭЦП электронную подпись.

5. Аудит и мониторинг (проверка БКИ)
Закажите выписку из Бюро кредитных историй (через Госуслуги это бесплатно дважды в год).

- Смотрите не только на выданные кредиты, но и на **запросы**.
- Если видите лавину запросов от МФО (как в списке выше) — значит, ваши данные попали в бомбер. Сами по себе запросы денег не крадут, но это сигнал: нужно мониторить ситуацию.

Один из 4х сайтов, которые я смотрел уже на следующие сутки

6. Цифровая криминалистика.
Прежде чем удалять чат у себя, сделайте **экспорт истории** или скриншоты.
В Telegram Desktop есть функция Export Chat History. Сохраните всё: ID ботов, никнеймы, номера телефонов, время сообщений. Возможно эти логи — единственное доказательство если дело дойдет до реального финансового ущерба. Факты лучше эмоций.

Заключение: почему это важно

Это не история о «глупости» или «доверчивости».
И точно не про «пожилых людей, которые плохо разбираются в технологиях». В этой истории нет ни одного примитивного хода. Здесь нет «переведи деньги», «назови код» или «безопасного счёта» в лоб. Здесь работает профессионально выстроенная цифровая атака, в которой человек — не слабое звено, а цель.

Это история о том, как ломают не через уязвимости в софте, а через уязвимости в привычках. Через то, что для нас кажется нормальным и безопасным:

- рабочий чат
- знакомые фамилии
- служебный тон
- «приказ сверху»
- формальные процедуры
- цифровые сервисы государства

С точки зрения IT это не взлом.
Это профессиональная социальная инженерия: сценарий, роли, тайминги, резервные планы, автоматизация. Настоящая модель, где пользователь — конечная точка, а его психика — интерфейс.

Сегодня это врач.

Завтра — бухгалтер с доступом к счетам.

Послезавтра — учитель с данными учеников.

Инженер. Кадровик. Айтишник. Любой, кто привык выполнять рабочие процессы и доверять «системе».

Важно понять главное: **мошенники больше не атакуют «человека вне социальной системы» — они атакуют человека *внутри* системы.**
Они не просят выйти из роли. Они используют её.

Единственный реальный барьер — знание сценария.

Если вы один раз увидели эту схему целиком:
рабочий чат → доверие → «техника» → шок → давление → изматывание
и она больше не работает так, как задумано. Магия исчезает.

Именно поэтому такие истории нужно фиксировать, разбирать и публиковать.
Не ради хайпа. Не ради жалости.

А ради того, чтобы в следующий раз — увидев знакомый шаблон — вы просто закрыли чат и прекратили диалог.

Автор: Михаил Шардин
🔗 Моя онлайн-визитка
📢 Telegram «Умный Дом Инвестора»

18 декабря 2025

Теги: развод, мошенничество, рабочий чат

Хабы: Информационная безопасность, Финансы в IT

256 Карма 92.1 Общий рейтинг

Михаил Шардин @empenoso

Автоматизация / Data & ML / Финансы / Smart Home

Подписаться

Сайт Сайт GitHub

Комментарии 168

Публикации

ЛУЧШИЕ ЗА СУТКИ ПОХОЖИЕ

David_Osipov
19 часов назад

Как «серый» бизнес Femida Search строит зомби-ферму внутри Хабра для обхода Песочницы

Простой 4 мин 11K

Репортаж

+77 16 51

monobogdan
8 часов назад

Как я на КПК оперативную память увеличивал [Длиннопост про железо]

Простой 6 мин 6.6K

Ретроспектива

+34 6 5

shadowform
4 часа назад

История о том, как я пытался подключиться к Starlink в России. История полная приключений

Средний 16 мин 4K

Из песочницы

+33 21 18

AlexeyPolunin
20 часов назад

Как я научился без скандалов выходить из зомби-проектов систем автоматизации

9 мин 8.7K

+32 31 6

Alekseyl
22 часа назад

Как мы сократили объем данных в 10 раз, не повредив пользовательскому опыту, или переезд Postgres → ClickHouse

Средний 13 мин 10K

Кейс

+29 39 7

HappyTalkie
9 часов назад

Как мы продавали компьютеры в 90-х. Часть #02

6 мин 4.4K

+20 1 5

DRoman0v
3 часа назад

Умное освещение в доме на базе Philips Hue. Личный опыт

7 мин 2.5K

+15 7 1

Laborant_Code
22 часа назад

От пустоты к идее: как я создал свою первую доску вдохновения

Простой 27 мин 6.9K

Обзор

+14 11 0

beeline_cloud
19 часов назад

«Галя, у нас замена»? Почему хайп со сменой программистов на системы ИИ — далеко не первая «паническая атака» в отрасли

7 мин 23K

Аналитика

+12 32 81

iMonin
18 часов назад

Как вихревая трубка Ранка-Хилша превращается в «Вихревой вакууматор»

11 мин 6.8K

+11 4 2

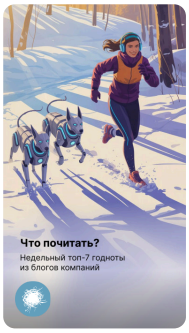
Упрощаем клиентский путь с помощью Цифрового профиля

Турбо

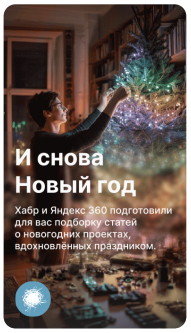
Показать еще

ИСТОРИИ

Год облака в подарок: 2 VM, БД, 100 ГБ



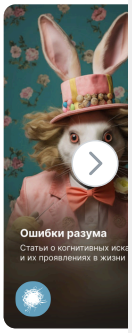
Годнота из блогов компаний



Через 3, 2, 1...

Работать без психологических проблем

Полезная подборка о зрении



Когнитивные искажения

ВАКАНСИИ

Frontend-разработчик React
от 150 000 ₽ · ДАЛЕЕ · Москва · Можно удаленно

Frontend-разработчик (Vue)
от 150 000 ₽ · ДАЛЕЕ · Можно удаленно

Ищем контент-менеджера на удалёнку (HoReCa проекты)
от 55 000 до 66 000 ₽ · ULHC · Можно удаленно

Хабр

Настройка языка

Техническая поддержка